Exhibit 37

XCP.Sony.Rootkit

Overview

Summary

XCP.Sony.Rootkit Extended Copy Protection(XCP) is Digital Rights Management (DRM) software manufactured by First4Internet, a UK company. This particular variant of XCP is licensed and bundled by Sony BMG, and is reportedly distributed on more than 2 million Sony BMG Audio CDs. This software is intended to stop casual CD piracy. Toward this end, the software is designed to prevent protected CDs being played with anything other than an included Media Player, Music Player.

See Also

XCP.Sony.Rootkit.Patch · Music Player ·

Category

Trojan : Any program with a hidden intent. Trojans are one of the leading causes of breaking into machines. If you pull down a program from a chat room, new group, or even from unsolicited e-mail, then the program is likely trojaned with some subversive purpose. The word Trojan can be used as a verb: To trojan a program is to add subversive functionality to an existing program. For example, a trojaned login program might be programmed to accept a certain password for any user's account that the hacker can use to log back into the system at any time. Rootkits often contain a suite of such trojaned programs.

Variants

XCP.Sony.SP2 ·

Reasons For Retention

Installs without user permission, presenting only a vague and misleading EULA
Changes system configuration without user permission at time of change.
Defends against removal of, or changes to, its components
Silently modifies other programs' information or website content as displayed.
Includes mechanisms to thwart removal by security or anti-spyware products.
Cannot be uninstalled by Windows Add/Remove Programs and no uninstaller is provided with application.

Origins

Author

First4Internet

Others By This Author

XCP.Sony.SP2 · XCP.Sony.Rootkit.Patch · XCP.Sony.SP2 · XCP.Sony.Rootkit.Patch ·

Vendor

Sony BMG

Date of Origin

June, 2005

Distribution

Distribution

When the CD is inserted, a EULA is displayed. This document contains reference to the installation of software on the machine, but does not give specific details, and in fact implies that the software can be uninstalled. If the user rejects the EULA, the CD is ejected and cannot be played. If the user accepts, XCP.Sony.Rootkit is installed on the user's machine. If autorun is not enabled, the cd still will not be playable except by Music Player.

Operation

General

XCP.Sony.Rootkit installs a DRM executable as a Windows service, but misleadingly names this service "Plug and Play Device Manager", employing a technique commonly used by malware authors to fool everyday users into believing this is a part of Windows. Approximately every 1.5 seconds this service queries the primary executables associated with all processes running on the machine, resulting in nearly continuous read attempts on the hard drive. This has been shown to shorten the drive's lifespan.

Furthermore, XCP.Sony.Rootkit installs a device driver, specifically a CD-ROM filter driver, which intercepts calls to the CD-ROM drive. If any process other than the included Music Player (player.exe) attempts to read the audio section of the CD, the filter driver inserts seemingly random noise into the returned data making the music unlistenable.

XCP.Sony.Rootkit loads a system filter driver which intercepts all calls for process, directory or registry listings, even those unrelated to the Sony BMG application. This rootkit driver modifies what information is visible to the operating system in order to cloak the Sony BMG software. This is commonly referred to as rootkit technology. Furthermore, the rootkit does not only affect XCP.Sony.Rootkit's files. This rootkit hides every file, process, or registry key beginning with sys. This represents a vulnerability, which has already been exploited to hide World of Warcraft RING0 hacks as of the time of this writing, and could potentially hide an attacker's files and processes once access to an infected system had been gained.

Sony BMG has released a patch which removes the rootkit and eliminates the above vulnerability. The patch fails the eTrust PestPatrol scorecard in its own right and its security advisor page can be found here. After the patch is run this variant of the XCP.Sony.Rootkit program still violates the eTrust PestPatrol Scorecard. The Patched program XCP.Sony.SP2's encyclopedia page can be found here.

Storage Required

Security Issues

XCP.Sony.Rootkit modifies you operating system at a low level, represents a large threat to both corporate and consumer users system integrity.

The Rootkit functionality hides files and enables hackers and other spyware to hide files with impunity.

Recommendations

Caution

Access to the user's CD-ROM will be disabled if XCP.Sony.Rootkit is removed manually, due to the missing filter driver. Reconfiguring the CD-ROM driver to a functioning state will be beyond the ability of the average home user. No uninstaller is included with XCP.Sony.Rootkit. Sony BMG has indicated that an uninstaller is available here. Analysis of the uninstaller has shown that it leaves significant vulnerabilities open after running. These vulnerabilities would allow hostile web sites to remotely execute code on a user's machine, among other things.

Detections:

List of Objects Present:

PestPatrol detects the following files and registry entries for this software..

Executable Files:

systemroot+\system32\$sys$upgtool.exe
systemroot+\system32\$sys$filesystem\$sys$drmserver.exe
systemroot+\cdproxyserv.exe
autorun.exe
go.exe

DLL Files:

systemroot+\system32\$sys$filesystem\unicows.dll
systemroot+\system32\$sys$filesystem\dbghelp.dll
systemroot+\system32\$sys$caj.dll
systemroot+\system32\tmpx\wnaspi32.dll
systemroot+\system32\tmpx\wnaspi.dll

Registry Items:

HKEY_CLASSES_ROOT\clsid\{78037074-0beb-496e-9e4c-92d92d562168}
HKEY_CLASSES_ROOT\clsid\{78037074-0beb-496e-9e4c-92d92d562168}\inprocserver32
HKEY_CLASSES_ROOT\clsid\{c62a2089-4eb1-4ebb-8635-0d1fcdd6bf25}
HKEY_CLASSES_ROOT\clsid\{c62a2089-4eb1-4ebb-8635-0d1fcdd6bf25}\control
HKEY_CLASSES_ROOT\clsid\{c62a2089-4eb1-4ebb-8635-0d1fcdd6bf25}\inprocserver32

Files:

systemroot+\system32\tmpx\wnaspi32.dll
systemroot+\system32\$sys$upgtool.exe
systemroot+\system32\drivers\$sys$cor.sys
systemroot+\system32\tmpx\apix.vxd
systemroot+\system32\tmpx\asplenum.vxd

Directories:

systemroot+\system32\$sys$filesystem

Research

File Analysis

- XCP.Sony.Rootkit

More Info

- Mark Russinovich of Sysinternals was the first (to our knowledge) to discover this rootkit. His blog entry is at http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html.

- AllTheWeb
- AltaVista
- AOL Search
- Ask Jeeves
- Google
- HotBot
- Lycos
- LookSmart
- MSN
- Yahoo!

Research By

- Stefan Berteau
- Computer Associates eTrust PestPatrol

How valuable was this information? Not at all ○ ○ ○ ○ ○ Extremely **Submit**